Voluntary Voting System Guidelines: Security and Transparency

Ronald L. Rivest, TGDC & Chair, STS
John Wack, NIST

EAC Standards Board Meeting (Denver)

August 24, 2005

Outline

- Introduction and overview (Rivest)
- Technical presentation (Wack)
  - Software Distribution & Setup Validation
  - Wireless
  - VVPAT
- Future Directions (Rivest)
  - IDV

Introduction

Ron Rivest

Introduction

- Thanks to: EAC, TGDC, STS Subcommittee, NIST, Experts, You
- High-level goal is to make your job easier, by
  - "raising the security bar" for system certification
  - making election results easier to certify and justify to skeptical public or losers
  - improving transparency

Voting System Security is Hard

- Computerization of voting systems gives us the headaches of ordinary computer security, plus
  - requirement that voter must not be given a receipt proving how he/she voted makes security much tougher.
- Now a major research area:
  - NSF just awarded $7.5M to a consortium of five institutions to research voting system security.

Voting – Potential Adversaries

- Anyone (voter, vendor, EO, pollworker) is potential adversary to voting system integrity and/or voter privacy.
- Important to review all potential threats.
- Important to understand that considering *A* as a potential threat not intended to imply that *A* is dishonest or actually intent on election fraud.
- Important to identify potential "single points of failure" and add mechanisms to mitigate risk.

Timeline

- Fall '04: Expert testimony, initial subcommittee meetings.
- Jan '05: TGDC resolutions passed
- Jan-Apr '05: NIST+TGDC work on VVSG
- April-June '05: VVSG approved by TGDC, delivered to EAC, published by EAC for comment.
- June 29—Sep 30 '05: Comment period.

Initial Issues Considered

- Wireless
- VVPAT
- Source code availability
- Documentation requirements
- "Tiger team" evaluations
- Best practices
- System logs

Initial Issues Considered (cont.)

- COTS
- Cryptography
- Standardized data formats
- Multiple stored ballots
- Software development standards
- Software distribution
- Setup validation

Initial Issues Considered (cont.)

- Remote voting
- Standardized computer security evaluation procedures
- Disclosure of evaluation results
- De-certification of systems
- Centralized evaluation and incident database
- …

TGDC passed resolutions

- Resolutions reflect consensus of TGDC on importance of various isssues, and near-term relevance. Provide guidance to NIST.
- #05-04: Currently certified voting software -> NSRL
- #12-05: Voter verifiability (IV/DV)
- #14-05: COTS software
- #15-05: Software Distribution
- #16-05: Setup Validation
- #17-05: "Tiger team" testing

TGDC passed resolutions

- #18-05: Documentation
- #21-05: Multiple ballot representations
- #22-05: Federal IT security standards
- #23-05: Common ballot formats
- #32-05: De-certification
- #35-05: Wireless

VVSG 2002 Revisions

- Current VVSG revises 2002 standards, and emphasizes (wrt security):
  - VVPAT (EAC guidance emphasized this)
  - Wireless
  - Software distribution and setup validation

Technical Presentation

John Wack, NIST

Future Directions

Ron Rivest

Future Directions

- Comprehensive revision/rewrite of VVSG.
- Coverage of aspects considered by TGDC, but for which no requirements yet written.
- Coverage of new aspects.
- Phase-In of new requirements determined by EAC.

Future VVSG May Include:

- IDV – Independent Dual Verification
- "Tiger Team" testing
- COTS
- Cryptographic Requirements
- Improved Documentation and Testing Requirements
- …

IDV – Independent Dual Verification

- Informative in current VVSG, part of new material in future versions
- IDV voting systems produce at least two ballot records, both verifiable by the voter and one unchangeable by voting system
- At least one record verifiable directly, or both verifiable by systems from different vendors
- Records usable in comparisons and audits
- Approach can improve resilience of voting systems to software attacks
- Needed as backup to more vulnerable computer-based ballot records

IDV

- Marketplace responding to IDV
- Systems available today that are in the IDV ballpark:
  - VVPAT
  - DRE add-ons – Witness
  - Some optical scan systems
  - Some crypto systems can be IDV
- Further work needed to specify requirements for IDV systems

"Tiger Team" testing

- Give a team of experts full rein to search for security vulnerabilities.
- They get full system documentation and access to system itself.
- "In order to defeat an adversary, you must think like an adversary."
- Further work needed to define team composition, level of effort, criteria for evaluating results.

COTS Software

- COTS software very useful, but may be buggy, produced overseas, or "black box" (no source code available for review).
- Further work needed to clarify when COTS software may be included in voting system, and how it is to be evaluated.

Cryptographic Requirements

- Cryptographic techniques, such as digital signatures and message authentication codes, can be used to improve system integrity and increase resistance to fraud.
- Further work is needed to specify what information transfers require such cryptographic protection.

Other Major Goals

- Stronger requirements for system documentation, including "public" section.
- Complete and comprehensive guideline with clear requirements and associated test methods for Voting System Testing Labs
- Strong core security section
  - Hardening and auditing requirements
  - Robust testing requirements
- Comprehensive threat analysis to drive overall security requirements
- Please let us know of your preferences/priorities!

For More Information…

- Ron Rivest
  - rivest@mit.edu
- John Wack
  - 301-975-3411, voting@nist.gov
- NIST Voting Site
  - Contains all NIST, TGDC documents, drafts, meetings, etc.
  - http://vote.nist.gov

(The End)